

Class Paper 5

Healthcare Simplification

THE EXECUTIVES

Authored by:

Joanne Leal

Stacey Branch

Jose Fonseca-Rivera

Krystyn Clark

John Gibbins

Thomas Luke

PMO 526 Health Services Organization

Department of Preventive Medicine and Biometrics

Uniformed Services University of the Health Science

26 October 2002

Healthcare Simplification

The Health and Insurance Portability and Accountability Act (HIPAA) was enacted to address several perceived shortcomings in the United States' health care system. Among its provisions is a mandate to streamline administrative and financial healthcare information systems. With the goal of increased administrative efficiency, HIPAA will purportedly save billions of health care dollars. This effort has been termed "healthcare simplification" with three broad aims: 1) Standardize electronic data by code sets to enhance information flow; 2) Create unique identifiers for payers, providers, employers and patients; and 3) Mandate the adoption of security standards to maintain patient privacy and confidentiality. A host of regulations, penalties and new oversight organizations have been instituted/proposed to enforce this process.

Clearly, standardization of electronic healthcare information systems will allow the industry to communicate more efficiently. A historical perspective is the creation of the National Institute of Technology and Standards (NITS) in 1901. This department was created to facilitate commerce by standardizing measurements and terminology. This allowed manufacturers in disparate locations to communicate critical data in a uniform fashion. Before the creation of NITS, the manufacturing industry utilized a hodgepodge of standards and nomenclatures in the description of even simple items like screws. The lack of standardization created confusion and error in the construction of complex machinery – a situation severely undermining the efficiency of an industrialized nation. For similar reasons, standardizing healthcare data and transmission is a logical step from the perspective of economics and business. Currently, a variety of insurance forms,

electronic programs, and user specific information are utilized. This situation results in system incompatibility making healthcare system management more difficult.

To effectively standardize personal and health related information, the data must be reduced into binary code, within a defined format, and be compatible to the various operating systems in use. Since patients have similar names, are mobile, and change jobs, correctly identifying an individual patient is difficult a difficult proposition in a country of 300 million. To address this issue, a unique digital identifier code will be assigned to each patient and healthcare organization within the healthcare system. This will allow rapid transmission of useful data from one organization to the next. In fact, an electronic portfolio can be created listing a patient's age, sex, weight, health history, utilization pattern, insurance carrier, and other demographic data.

Privacy and Confidentiality

Standardization of health information has some inherent risks. Though private health information has always had the potential for abuse, traditional non-standardized information transfer made it difficult to access, collect, and interpret. A standardized system clears away much of the difficulty in collecting this information if access to the system can be obtained. Unauthorized users could potentially identify patients with particular illnesses or risk factors. If a particular patient is "uniquely" known, and is likely to pose an economic burden to his employer or insurance carrier, his prospects for employment or medical insurance could be jeopardized.

To protect patients, the "HIPAA Security Rule is designed to provide protection for all individually identifiable information that is maintained, transmitted, or received in electronic form" (Tricare Management Activity, February 2002) to include written and

verbal communication. This rule covers administrative procedures, physical safeguards, and technical security services and mechanisms. Civil penalties for violations of this regulation include fines and/or imprisonment for security lapses and breaches. The regulation covers payers, information clearinghouses, and providers who transmit health data electronically. This is not merely a theoretical concern as private healthcare information has been used to identify patients to ill effect.

Impact and Challenges

Since this standardized data system will contain high quality information of great economic benefit to a variety of businesses, insurers, employers, and others, we believe that it is unavoidable that some will attempt unauthorized access to the data. One considerable obstacle to safeguarding the system is that hundreds of thousands of individuals must have access to the system to input and retrieve patient data. Securing such a system is extremely difficult. Though easy to deny access to someone with a passing knowledge of computer science, true experts in the field of computer information systems are likely to covertly circumvent any user-friendly system. Standardization may allow the collection of accurate private health information on a scale not possible with a de-centralized system.

Additionally, HIPAA has created a legal expectation of privacy and confidentiality to the consumer. Since torts can be filed to right wrongs, it is likely that private and class action lawsuits will be filed seeking redress when patient information is compromised. The cost could be considerable in direct judgements and legal fees. As important, risk managers are likely to implement strict compliance procedures within their organization that will impose a considerable administrative and financial burden to

their organization. This hidden cost of administering healthcare is likely to have a negative impact of the delivery of healthcare to the consumer, the provider and administrators.

A standardized system of transmitting data will ease some administrative burden. This is particularly true of bureaucratic end users like the state and federal governments. We are not sure that HIPAA will lead to healthcare simplification at the provider, hospital, insurer and HMO level. This law is extremely complicated and implementing tough “confidentiality” requirements will require significant oversight. In the best of situations, existing personnel will be able to safeguard and manage these new requirements. More likely, additional personnel will be required to manage the system. Conversely, additional administrative tasks may be shifted to doctors and nurses to make HIPAA compliance possible - effectively hiding the true administrative cost incurred. If the burden of additional administrative and management tasks are shifted to providers, this could have a negative impact on patient access and quality of care.

Though HIPAA allows providers to communicate confidential patient information in the context of their duties, many clinicians are concerned that this law will inhibit their ability to seek advice and assistance from colleagues, peers, and secondary health professionals. We note that many prominent physicians and healthcare professionals, including Dr. Zimble, are extremely concerned about the unexpected impact this law may have on patient care and medical research. The issue is quality of care, and the value of differing viewpoints surrounding a patient’s care and the collegial history of doctors proffering advice to their peers. Despite HIPAA’s protective exclusions, physicians are highly concerned with litigation and the potential damage inflicted on their careers and

reputation should they be investigated or accused of exceeding the limits of patient confidentiality. Even a subtle withholding or hesitancy in discussing patient care with another health professional may have a profound impact on the care and ultimate outcome of an individual patient.

Similarly, healthcare administrators have a very difficult task. Not only must they collect data, but secure the cooperation of the organization, design new systems, retrain personnel, and receive and transmit the data in a secure and legally defensible manner. We are struck by the advice contained in one TRICARE management bulletin that invokes this “golden rule” to administrators implementing the HIPAA security rule: “*You must document everything!* What is documented must reflect what you actually do and it must be kept current and accurate.” From this viewpoint, we recognize that the administrative burden must increase to comply with this internal directive. A skeptic might note that healthcare simplification is a misnomer.

We believe that patient confidentiality is important but should not be mistaken for patient healthcare. Standardizing codes and improving the electronic transmission of data will lead to better efficiency in some aspects of the healthcare system. However, a centralized system of high quality patient data lends itself to abuse and may in fact allow harmful breaches in patient confidentiality. We believe that the addition of numerous regulations designed to protect patient confidentiality recognizes the potential weakness of a standardized data system. After careful consideration, we do not believe that HIPAA can result in a net simplification of the healthcare system. We also predict long-term administrative and compliance costs associated with strictly protecting patient confidentiality. Further, we sense that:

1. Providers are wary of a system that may limit the free flow of medical advice and informal consultation between physicians.
2. Healthcare administrators have no choice but to comply with HIPAA and are responsible for maintaining secure data that is utilized, modified and accessed by numerous users. Highly secure data may not be possible in practice and managing such a system is likely to be extremely difficult and unrelated to providing the best care possible.
3. Patients will continue to utilize the healthcare system but the right of confidentiality will impact access, cost and quality of care.

Finally, we believe that HIPAA will have unforeseen consequences best evaluated once the system is in widespread use. Experience shows that complex regulatory mandates tend to become more restrictive and burdensome over time. We expect future modifications to correct currently unforeseen problems within the system, or to implement ideological political or sociological precepts, will have the potential to create continuing administrative problems.